DOI https://doi.org/10.15589/znp2019.1(475).13
УДК 004.054

FORMATION OF A COMPREHENSIVE STRATEGY FOR MANAGING THE RISKS OF QUALITY, INFORMATION SECURITY AND THE INTEGRITY OF GXP-CRITICAL DATA AUTOMATICALLY

ФОРМУВАННЯ КОМПЛЕКСНОЇ СТРАТЕГІЇ УПРАВЛІННЯ РИЗИКАМИ ЯКОСТІ, ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЦІЛІСНОСТІ GXP-КРИТИЧНИХ ДАНИХ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Serhii V. Medushevskiy
victorovich.med@gmail.com
ORCID: 0000-0002-9371-0428

С. В. Медушевський,
викладач

Cherkasy Bohdan Khmelnytsky National University, Cherkasy
Черкаський національний університет імені Богдана Хмельницького, м. Черкаси

Abstract. The **purpose of the article** was to increase the effectiveness of risk management in the process of automated information system (AIS) validation, including the risks of information security and integrity of GxP-critical data, by forming an effective strategy that takes into account the basic risk management tactics in project management automation as well as the industry specificity of the pharmaceutical industry.
Method. The analysis of publications has made it possible to define as one of the most important stages of the process of risk management in projects on automation of production processes the development of the concept (strategy) of managing these risks.
Results. The article raises the problem of information risk management in the projects of implementation of AIS in the pharmaceutical industry. The definition of a risk response strategy first depends on the nature and characteristics of the risk itself. The elements of the information security risk management strategy and the integrity of GxP-critical data are considered and the principles necessary for the development and implementation of the risk management strategy at the pharmaceutical enterprise are highlighted. It is determined that the proposed approach to risk management uses a systematic approach to AIS and related implementation projects, since AIS are modular systems in structure and often hierarchical. To determine performance criteria for the AIS function, there are three levels of significance for variability. In the course of the analysis, the main risk attributes in the AIS validation project are highlighted, which are the basis for their classification and formation of the risk management strategy. Phases of the iterative process of automation of pharmaceutical production are considered.
Scientific novelty. Guidelines are provided to manage the risks of information security and the integrity of AIS-data and to simplify the analysis process.
Practical importance. The result is a well-grounded solution to the problem of forming an information security risk management strategy and the integrity of GxP-critical data that emerges in the AIS validation process. Conceptual frameworks are developed for creating an effective risk management strategy in AIS validation projects.

Key words: automation; validation; information system; risks; GxP-data.

Анотація. Метою статті було підвищення ефективності управління ризиками в процесі валідації автоматизованої інформаційної системи (далі – АІС), в тому числі ризиками інформаційної безпеки та цілісності GxP-критичних даних, шляхом формування ефективної стратегії, яка враховує базову тактику ризик-менеджменту в управлінні проєктами автоматизації, а також галузеву специфіку фармацевтичної промисловості.
Методика. Проведений аналіз публікацій дозволив як основне завдання дослідження визначити один з найважливіших етапів процесу управління ризиками в проєктах з автоматизації виробничих процесів – вироблення концепції (стратегії) управління цими ризиками.
Результати. У статті підіймається проблема управління інформаційними ризиками проєктів впровадження (АІС) на фармацевтичному виробництві. Визначення стратегії реагування на ризик залежить від характеру і характеристик самого ризику. Розглянуто елементи стратегії управління ризиками інформаційної безпеки та цілісності GxP-критичних даних та виділено принципи, необхідні при розробці та реалізації стратегії управління ризиками на фармацевтичному підприємстві. Визначено, що пропонований метод управління ризиками використовує системний підхід до АІС і пов'язаних з ними проєктів впровадження, оскільки АІС є модульни-

ми системами за структурою і часто є ієрархічними. Для визначення критеріїв ефективності виконання функції АІС виділяють три рівні значущості за варіабельністю.
В ході аналізу були виділені основні атрибути ризиків у проєкті валідації АІС, які є основою для їх класифікації та формування стратегії управління ризиками. Ми розглянули фази ітеративного процесу автоматизації фармацевтичного виробництва.
Наукова новизна. Запропоновано методичні рекомендації для управління ризиками інформаційної безпеки та цілісності даних АІС та з метою спрощення процесу аналізу.
Практична значимість. Результатом є обґрунтоване рішення задачі формування стратегії управління ризиками інформаційної безпеки та цілісності GxP-критичних даних, що виникають в процесі валідації АІС. Були розроблені концептуальні засади для створення ефективної стратегії управління ризиками в проєктах валідації АІС.

Ключові слова: автоматизація; валідація; інформаційна система; ризики; GxP-дані.

ПОСТАНОВКА ЗАДАЧІ

Розробка та впровадження автоматизованої інформаційної системи на фармацевтичному виробництві є складним процесом, що вимагає від учасників впровадження (замовника і виконавця) максимальних зусиль для досягнення позитивного результату [1].

У забезпеченні надійного функціонування АІС і досягненні необхідного рівня безпеки та цілісності GxP-критичних даних особливу роль відіграє процес управління ризиками при її проєктуванні, розробці, впровадженні, валідації та експлуатації.

Проблема управління інформаційними ризиками АІС є комплексним завданням, що включає низку таких напрямів: формування узгодженого поняття про рівень прийнятного ризику; оцінку актуального стану ризиків в трьохвимірному просторі координат «тяжкість наслідків – ймовірність виникнення – ймовірність виявлення»; пошук прийнятних заходів щодо зниження рівня ризику до допустимих значень; розробку і реалізацію необхідних коригувальних і запобіжних дій.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Управління ризиками – це процес ідентифікації та аналізу ризиків з подальшим прийняттям рішень про коригувальні та запобіжні дії, спрямованих на мінімізацію ризикових подій, зниження ймовірності виникнення несприятливого результату, а також мінімізацію негативних наслідків і можливих втрат.

Попри значний масив робіт теоретичного та практичного характеру, спостерігається дефіцит комплексних досліджень в галузі побудови системи ризик-менеджменту в управлінні проєктами з автоматизації фармацевтичних виробництв. У дослідженні [2] автором аналізуються різні підходи до організації функціоналу проєктних організаційних структур, виділяються основні функції в рамках управління ризиками. Наявні моделі систем захисту інформації та методи оцінки ризиків порушення критично важливих властивостей захисту ресурсів майже не відображають специфіку систем захисту інформації як складних організаційно-технічних систем [3]. Для успішного аналізу ризиків необхідно проводити якісну ідентифікацію ризиків. Основою ідентифікації ризиків є їх класифікація [4].

Одним з найважливіших етапів процесу управління ризиками в проєктах з автоматизації виробничих процесів є вироблення концепції (стратегії) управління цими ризиками. При цьому формування стратегії, як правило, базується на виборі національних і міжнародних керівних документів і стандартів в галузі управління ризиками.

За основу для вирішення даної проблеми взято узагальнену онтологічну модель оцінки і управління інформаційними ризиками [5], що дозволяє цілеспрямовано вивчати взаємозв'язок основних концептів ризик-менеджменту в різних предметних галузях, зокрема у фармацевтичній промисловості.

Виявлені автором роботи [6] особливості управління ризиками інформаційної безпеки свідчать про високий рівень структурної складності даного процесу, реалізація якого не може обмежуватися чотирма послідовно виконуваними етапами (оцінка факторів ризику, оцінка ризику, оцінка співвідношення контрзаходів і можливого збитку, реалізація управління ризиками).

ВІДОКРЕМЛЕННЯ НЕ ВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ

Процедура з управління ризиками досить глибоко інтегрується в систему управління життєвим циклом АІС [7]. Оцінка і управління ризиками, що виникають в процесі валідації АІС, являє собою складний, слабко структурований та недостатньо формалізований вид діяльності.

Питання формального опису процесу управління ризиками в рамках валідації АІС залишаються сьогодні недостатньо опрацьованими в зв'язку з тим, що даний процес має низку специфічних особливостей. Це знижує ефективність управління інформаційними ризиками. Завдання оцінки і управління рівнем ризиків має низку специфічних особливостей, пов'язаних зі слабкою структурованістю і наявністю як об'єктивних, так і суб'єктивних невизначеностей.

Мета дослідження – підвищення ефективності управління ризиками в процесі валідації АІС, в тому

числі ризиками інформаційної безпеки та цілісності GxP-критичних даних, шляхом формування ефективної стратегії, яка враховує базову тактику ризик-менеджменту в управлінні проєктами автоматизації, а також галузеву специфіку фармацевтичної промисловості.

МЕТОДИ, ОБ'ЄКТ ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

Методи дослідження базуються на положеннях теорії системного аналізу, концепції загального управління якістю (TQM), статистичних методах управління якістю, теорії прийняття оптимальних рішень, кількісних і якісних методиках оцінки ризиків. Об'єктом дослідження є ризики, що виникають в процесі валідації АІС. Предметом дослідження є моделі, методики та алгоритми управління ризиками, що виникають в проєктах автоматизації фармацевтичних виробництв.

ОСНОВНИЙ МАТЕРІАЛ

Загальні принципи процесу управління ризиками базуються на результатах оцінки ризику, техніко-технологічному та економічному аналізі потенціалу та середовища функціонування АІС. Управління ризиками включає в себе розробку стратегії і тактики.

Стратегія управління ризиками інформаційної безпеки та цілісності GxP-критичних даних повинна складатися з набору різних методів і забезпечувати такі критерії ефективності: максимізувати узгодженість і адекватність оцінок факторів ризику, адаптивність до якісних даних; мінімізувати суб'єктивність і невизначеність оцінки ризику; враховувати неоднакову чутливість ризику до різних факторів.

Основні етапи процесів управління ризиками такі:

- контекстний аналіз, який включає в себе розуміння інтересів і середовища, виявлення різних зацікавлених сторін, встановлення основи, на якій будуть аналізуватися ризики, і планування процесів управління ризиками;
- ідентифікація ризику, тобто виявлення та перерахування загроз, небезпек та інших негативних проблем, які можуть вплинути на АІС;
- якісний аналіз ризиків, тобто документування характеристик ризиків, аналіз їх впливу на АІС і розуміння їх взаємозв'язків;
- кількісна оцінка ризиків, тобто оцінка ймовірності виникнення ризиків і чисельна оцінка їх впливу на АІС;
- реагування на ризики, тобто планування та розробка варіантів і дій для запобігання або зменшення негативного впливу ризиків на АІС і посилення їх позитивного впливу.

Виділимо принципи, необхідні при розробці та реалізації стратегії управління ризиками на фармацевтичному підприємстві. Це баланс відповідальності та ініціативи, поєднання аналітики і ризикової евристики, багатоваріантність, проактивність, системність, безперервність.

Кількісний аналіз, який базується на інструментарії теорії ймовірності та математичної статистики, складається в числовому вимірі з впливу змін ризикових факторів проєкту на зміну ефективності проєкту і спирається на базисний варіант бізнес-плану проєкту автоматизації і проведений якісний аналіз. За ідентифікацію всіх можливих ризиків відповідає якісний аналіз, який визначає фактори ризику, послідовність робіт, під час виконання яких виникає ризик.

З системної точки зору пропонований підхід до управління ризиками передбачає, що АІС і процеси її реалізації можуть бути розділені на компоненти різних сегментів і рівнів. Отже, відбувається вплив факторів ризику безпосередньо на ці компоненти або взаємодія між компонентами, а потім це відображається у кінцевих результатах реалізації. Фактори ризику впливають на успіх окремих компонентів і, якщо вплив є досить негативним, можуть викликати помилки або збої, які впливають на інформаційну безпеку та цілісність GxP-критичних даних. Крім того, ймовірність і серйозність потенційної втрати є двома найбільш важливими змінними при виборі реакції на ризик і стратегії розробки коригувальних дій.

Пропонований підхід до управління ризиками використовує системний підхід до АІС і пов'язаних з ними проєктів впровадження, оскільки АІС є модульними системами за структурою, які часто є ієрархічними. Основне обґрунтування цього полягає в тому, що на компоненти АІС накладається вплив ризиків, а накопичення або конкретна комбінація відмов компонентів призводить до збою використання АІС в цілому.

Ефективний аналіз ризиків передбачає поєднання формалізованого підходу і емпіричних методів (ICH Q9). При правильному використанні він може служити ефективним інструментом, що дозволяє виявити джерела ризиків і найбільш критичні фактори, оцінити і запобігти можливим проблемам, заощадити ресурси і досягти більш високої якості використання АІС. Дуже важливою при цьому є наявність досвіду і практики, які дозволяють, з одного боку, використовувати перевірені і відпрацьовані схеми і підходи, а з іншого – виважено і продумано підходити до їх застосування в кожному конкретному випадку.

Для проведення валідації АІС повинні бути визначені за допомогою аналізу ризиків та задокументовані в протоколі валідації критичні стадії і операції автоматизованого процесу, а також контрольовані параметри для них. Результатом аналізу ризиків при цьому є визначення контрольних точок і параметрів, які повинні бути протестовані в процесі валідації.

Ітеративний проєкт з автоматизації фармацевтичного виробництва можна представити певними фаза-

ми. Для даного проєкту була побудована архітектура процесу розробки, зокрема і процес управління ризиками. Відповідно до методології RUP проєкт був розбитий на 5 фаз, що складаються з ітерацій (Рис. 1).

Кожна ітерація має такі підпроцеси: моделювання бізнес-процесів, управління вимогами, аналіз і проєктування, розробка, тестування, впровадження, конфігураційне управління, управління життєвим циклом АІС та управління середовищем (підтримка виробничого середовища).

Важливо розуміти, що функціональний аналіз об'єкта дослідження проводиться з метою перерахування, опису характеристик і класифікації всіх експлуатаційних функцій АІС поряд з фазами життєвого циклу [8]. Функціональний аналіз, зазвичай викладений в функціональних специфікаціях, є необхідною умовою, адже дозволяє валідаційній команді отримати однакове і вичерпне уявлення про об'єкт аналізу, тобто АІС, правильно визначити всі можливі види, наслідки і причини потенційних дефектів, помилок, збоїв об'єкта аналізу.

Рис. 1. Фази проєкту автоматизації процесів фармацевтичного виробництва

Для визначення критеріїв ефективності виконання функцій (характеристик АІС) використовується поняття варіабельності. Зазвичай виділяють три рівні значущості (за варіабельністю):

- клас 1 – нульова варіабельність, тобто ситуація, коли відхилення не допускаються (висока значимість);
- клас 2 – рівень, що допускає мінімальну варіабельність (мало відхилень), – середня значимість;
- клас 3 – рівень, що допускає певну варіабельність (можуть бути відхилення в певній кількості), – низька значимість.

Управління ризиками в проєкті валідації АІС починається з процедури їх ідентифікації. Ідентифікація ризиків є ітеративним процесом, де першу ітерацію може зробити команда управління проєктом, другу – інші учасники, остаточну – зовнішні щодо проєкту фахівці або безпосередньо користувачі. Ідентифікація ризиків проводиться систематично за допомогою контрольних таблиць, опитувальників при проведенні зборів і співбесід, а також через рецензування планів проєктів і процесів.

У результаті ідентифікації визначаються дискретні події, які можуть вплинути на проєкт автоматизації (ризики), а також дії, які можуть зробити ризики більш імовірними (умови ризиків). До основних вихідних даних, необхідних для ідентифікації ризиків, належать такі: опис мети проєкту, технічне обґрунтування, план проєкту, склад і послідовність робіт з розробки та валідації, плани для суміжних робіт, план управління якістю, а також договір на технічну підтримку АІС.

У ході аналізу були виділені основні атрибути ризиків в проєкті валідації АІС, які є основою для їх класифікації та формування стратегії управління ризиками. За допомогою класифікації ризики систематизується на підставі будь-яких ознак і критеріїв, що дозволяють об'єднати підмножини ризиків. Обґрунтована класифікація ризику сприяє чіткому визначенню місця кожного ризику в загальній системі і створює потенційні можливості для ефективного застосування відповідних прийомів управління ризиками.

Після ідентифікації, аналізу та оцінки ризиків необхідно скласти план управління ризиками, здійснювати моніторинг і застосовувати відповідні контрзаходи. При плануванні необхідно розробити контрзаходи для кожного з ризиків. Ослаблення впливу ризиків може бути досягнуте кількома такими шляхами: уникненням ризику, контролюванням ризику, перенесенням ризику і прийняттям ризику. Підсумковий план описує підхід і способи для вирішення ризику. Моніторинг ризиків, який необхідно проводити на всіх етапах життєвого циклу АІС, полягає в спостереженні за індикаторами ризиків для прийняття рішень щодо застосування плану реагування на ризики. Вхідними даними для процесу моніторингу є сценарії ризиків, порогові значення і поточний статус ризиків.

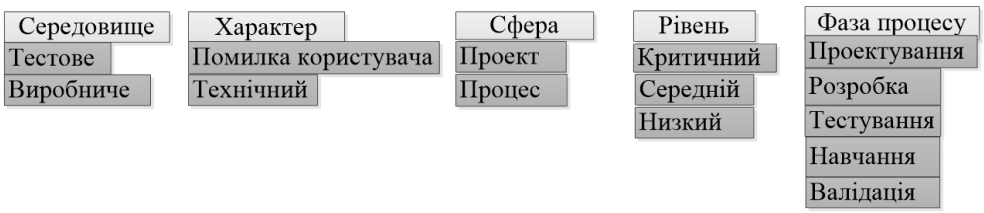

Рис. 2. Атрибути ризиків

ОБГОВОРЕННЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ

Запропонований підхід покликаний допомогти краще зрозуміти, як відбувається управління ризиками інформаційної безпеки та цілісності GxP-критичних даних при впровадженні AIC, а також з'ясувати, які чинники ризику є основними причинами збою. Цей підхід надає інструменти для ефективного реагування на ризики і пом'якшення їх наслідків у процесі впровадження та валідації AIC.

Формулювання і реалізація таких стратегій залежать від імовірностей ризиків і від зв'язку між конкретними подіями ризику, відмовою від компонентів і відмовою від використання AIC. Критичні компоненти і критичні події ризику повинні бути пріоритетами управління ризиками. Форма критичних компонентів AIC і подій критичного ризику в отриманих уявленнях стратегії, особливо в мінімальному наборі зрізів, надає важливу інформацію про уразливість проєкту впровадження і валідації AIC. В цілому мета стратегій – уникнути, передати, повністю зберегти або зменшити ризики.

ВИСНОВКИ

Загальним підсумком роботи є науково обґрунтоване вирішення задачі формування стратегії управління ризиками інформаційної безпеки та цілісності GxP-критичних даних, що виникають в процесі валідації AIC, і управління їх рівнем на основі фактичних даних. Розроблено концептуальні засади для створення ефективної стратегії управління ризиками в проєктах валідації AIC. Стратегія дозволяє в умовах суб'єктивної невизначеності вибрати оптимальну тактику управління ризиками з метою підвищення рівня інформаційної безпеки.

REFERENCES

[1] Medushevskyi S.V., Yefimenko N.A. (2017). Upravlinnia ryzykamy yakosti avtomatyzovanoi informatsiinoi systemy. [Tekhnichni nauky]. Visnyk Cherkaskoho derzhavnoho tekhnolohichnoho universytetu, no. 1, pp. 118-123. [in Ukrainian].

[2] Yslamova S.T., Kachanova E.A. (2019). Rysk-menedzhment v korporatyvnoў systeme upravlenyia proektam. Vestnyk Cheliabynskoho hosudarstvennoho unyversyteta, no. 7(429), pp. 124-130. [in Russian].

[3] Bratchenko A.Y., Butusov Y.V., Kobelian A.M., Romanov A.A. (2019). Prymenenye metodov teoryy nechetkykh mnozhestv k otsenke ryskov narushenyia krytychesky vazhnikh svoistv zashchyshchaemikh resursov avtomatyzyrovannikh system upravlenyia. Voprosi kyberbezopasnosty, no 1(29), pp. 18-24. [in Russian].

[4] Beliakov S.Y., Shabalkyn B.V. (2019). Rysky v upravlenyy proektamy developmenta. Moskovskyi ekonomycheskyi zhurnal, no. 8, pp. 811-818. [in Russian].

[5] Vibornova, O. (2017). Upravlenye ryskamy obrabotky ynformatsyy na osnove ekspertnikh otsenok [Information processing risk management based on expert judgment]. *Extended abstract of candidate's thesis*. Astrakhan: FHBOU VO KHTU [in Russian].

[6] Mykov, D. (2018). Upravlenye ynformatsyonnimy ryskamy v systemakh dystantsyonnoho monytorynha sostoianyia obiekta [Information risk management in remote monitoring systems]. *Extended abstract of candidate's thesis*. Moskva: FHBOU VO MHTU [in Russian].

[7] Medushevskyi S.V. (2018). Rozrobka unifikovanoi metodyky otsinky ryzykiv u protsesi validatsii avtomatyzovanykh informatsiinykh system. Tekhnichni nauky ta tekhnolohii, no 2, pp. 151-158. [in Ukrainian].

[8] Paniukov D.Y., Paniukova E.V. (2015). Predvarytelnoe yssledovanye obiekta analyza v ramkakh metoda FMEA. Ynnovatsyonnaia nauka, no 11, pp. 103-108[in Russian].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Медушевський С.В., Єфіменко Н.А. Управління ризиками якості автоматизованої інформаційної системи. *Вісник Черкаського державного технологічного університету. Серія «Технічні науки».* 2017. № 1. С. 118–123.

[2] Исламова С.Т., Качанова Е.А. Риск-менеджмент в корпоративной системе управления проектами. *Вестник Челябинского государственного университета.* 2019. № 7 (429). С. 124–130.

[3] Братченко А.И., Бутусов И.В., Кобелян А.М., Романов А.А. Применение методов теории нечетких множеств к оценке рисков нарушения критически важных свойств защищаемых ресурсов автоматизированных систем управления. *Вопросы кибербезопасности*. 2019. № 1 (29). С. 18–24.

[4] Беляков С.И., Шабалкин Б.В. Риски в управлении проектами девелопмента. Московский экономический журнал. 2019. № 8. С. 811–818.

[5] Выборнова О.Н. Управление рисками обработки информации на основе экспертных оценок : автореф. дисс. … канд. техн. наук. Астрахань : КГТУ, 2017. 24 с.

[6] Миков Д.А. Управление информационными рисками в системах дистанционного мониторинга состояния объекта : автореф. дисс. … канд. техн. наук. Москва : МГТУ, 2018. 18 с.

[7] Медушевський С.В. Розробка уніфікованої методики оцінки ризиків у процесі валідації автоматизованих інформаційних систем. *Технічні науки та технології*. 2018. № 2. С. 151–158.

[8] Панюков Д.И., Панюкова Е.В. Предварительное исследование объекта анализа в рамках метода FMEA. Инновационная наука. 2015. № 11. С. 103–108.